NCDOR

Next

Click Next to begin

Role-based Security Training for Technical Users

North Carolina
Department of Revenue

Introduction

Click Next to continue.

Back Next

This training item utilizes both voice-over functionality, as well as closed caption access. This way, this training module can be used either with or without audio.

Role-based Security Training for Technical Users

North Carolina
Department of Revenue
2015

Objectives

At the end of this module, you should be able to:

- Explain the importance of Rolebased Security for Technical Users
- Identify the required target audience
- Describe the technical security policies
- Define training based on your job role or duty
- Provide Tips for Detecting Insider Threats

Rolebased Security

Required by the IRS in Publication 1075 in Section 9.3.2.3.

Agencies are required to "provide individualized training to personnel based on assigned security roles and responsibilities."

Rolebased Security

Required for the following DOR Staff regardless of employment status (permanent, temp. or contractors):

- Entire IT Division
- Purchasing Division
- Internal Audit Division

Technical Security Policies

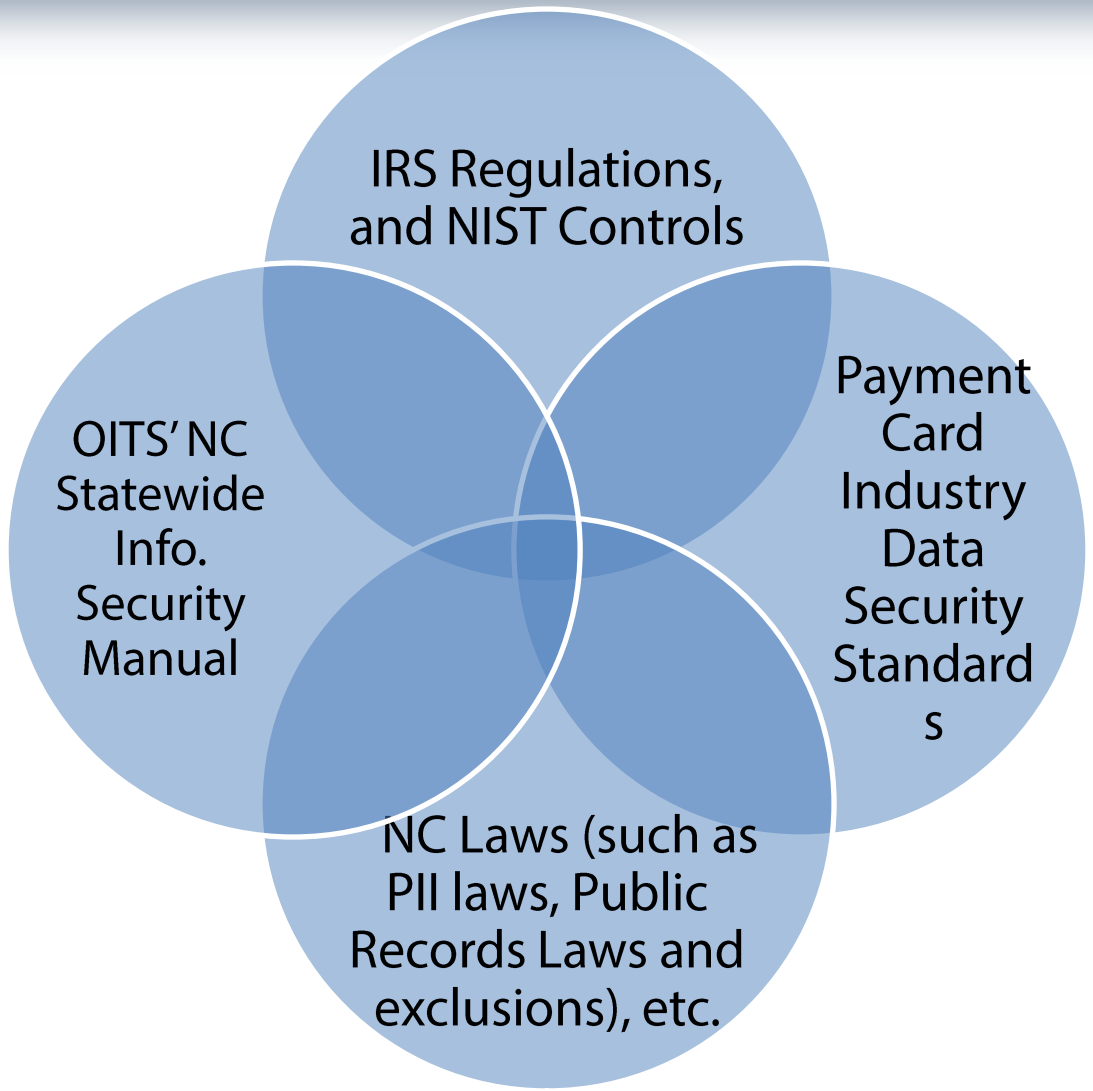
NIST Controls

- National Institute of Standards and Technology (NIST) was founded in 1901
- Part of the US Department of Commerce
- Provides best practices on security
- Updated Revenue Security Policy Manual is based on NIST Controls
- Revised policy numbers are tied to NIST Control Family numbering scheme for cross-referencing ease

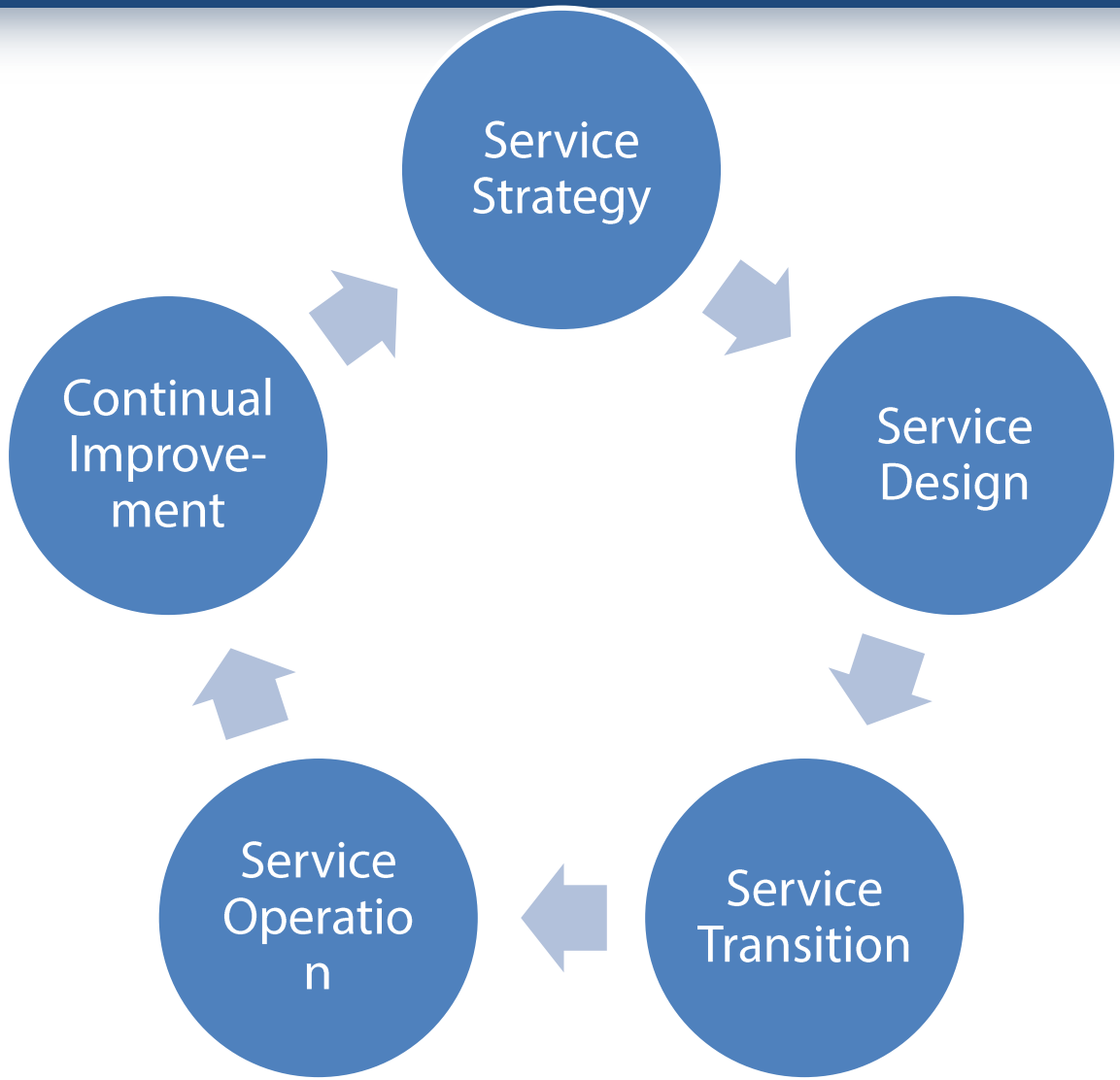
Importance of Policy Review

- Review the entire Security Policy Manual, including the Technical Security Policies.
- Refer any Security Policy Manual or Technical Security Policies questions to our Chief Information Security Officer.
- Technical User may frequently need to reference the Technical Security Policies section of our Security Policy Manual.

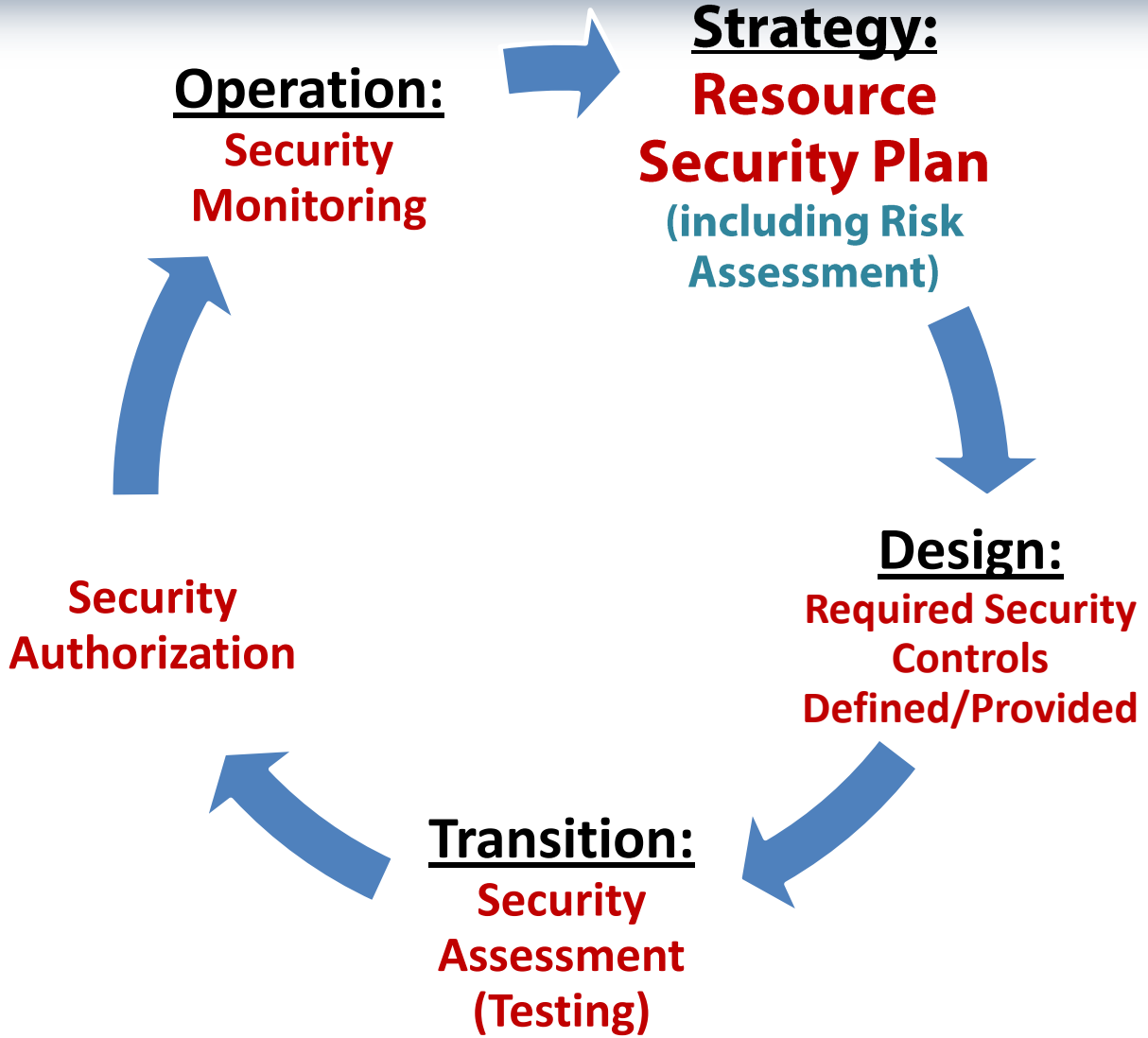
What influences DOR's Security Policies



ITIL Stages in a System Development Life Cycle (SDLC)



How Security fits into ITIL and SDLC



Technical Security Policy Category Listing

Major security control families within the Technical Security Policies section of Revenue's Security Policy Manual:

Abbreviation	Title of Security Control Family
AC	Access Control
AT	Awareness & Training
AU	Audit & Accountability
CA	Security Assessment & Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification & Authorization
IR	Incident Response
MA	Maintenance

Technical Security Policy Category Listing (cont'd)

Major security control families within the Technical Security Policies section of Revenue's Security Policy Manual:

Abbreviation	Title of Security Control Family
MP	Media Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	Resource & Service Acquisition
SC	Resource & Communication Protection
SI	Resource & Data Integrity
PM	Program Management

Technical Security Policy Category Listing (cont'd)

Follow Revenue Security Policies for developing and implementing information systems or changes

Information Technology staff , including the Information Security Division may frequently access policies

Remember that compliance with all Revenue Security Policies is a condition of your employment (or contract).

Rolebased Training

This Training is designed for:

This rolebased training is designed specifically for persons with the following roles or duties within NCDOR:

- Enterprise architects
- Information system developers
- Software developers
- Acquisition/procurement officials
- Information system managers
- System/network administrators
- Personnel conducting configuration management and auditing activities
- Personnel performing independent verification and validation activities
  security control assessors
- Personnel having access to system-level software

Categories of Job Functions Covered in this Training

Job Function Categories

- Manage
- Design
- Implement
- Evaluate

Manage Function

Manage – Revenue staff (i.e. Managers, supervisors, team leads, and project managers) responsible for managing staff and/or agency projects.

Role-specific security best practices affecting person with the "management" role as defined in NIST 800-16.

Security Best Practices for IT Project Managers

- *"Bake-in" Project Security*
- *Develop Project Charter*
- *Identify Stakeholders*
- *Plan Communications*
- *Plan Risk Management*
- *Secure Communications*
- *Authentication and Password Management*
- *Access Management*

Source: SANS Institute

Security Best Practices for IT Project Managers (cont'd)

- ***Encryption***
- ***Wireless Attacks***
- ***Physical Security***
- ***Secure Deliverables***
- ***Verify Deliverables (Operational hand-off)***
- ***Document Lessons Learned***

Design Function

Design – Revenue staff (i.e. system developers, engineers, etc.) responsible for the design of project activities.

Role-specific security best practices affecting person with the "Design" role as defined in NIST 800-16.

Security Best Practices for System Developers

- **Trust User Input at Your Own Peril**
- **Protect Against Buffer Overruns**
- **Prevent Cross-site Scripting**
- **Don't Require System Administrator Permissions**
- **Never create your own Encryption Code**

Source: MSDN Magazine (articles related to developing secure code)

Security Best Practices for System Developers (cont'd)

- Reduce Your Attack Profile
- Employ the Principle of Least Privilege
- Pay Attention to Failure Modes
- Impersonation is Fragile
- Fix Old Code First
- Automate (where possible)

Implement Function

Implement – Revenue staff who execute implementation (e.g., system administrators, network administrators).

Role-specific security best practices affecting person with the "Implementation" role as defined in NIST 800-16.

Security Best Practices for System Administrators

Authentication and Authorization

- **Remove or disable accounts upon loss of eligibility**
- **Use unique passwords for administrator accounts (different from your non-privileged accounts)**
- **Avoid Risky Behavior when using your Administrator Accounts**

Security Best Practices for System Administrators

Authentication and Authorization (cont'd)

- **When we say *"Avoid Risky Behavior when using your Administrator Accounts"*, we mean avoid the following actions while connected to your privileged account with Administrator rights.**

- **If you get infected with a system intruder, virus, worm or ransomeware, etc. while using your Administrator account, it could run with Administrator rights and propagate to mapped drives and servers. This could cause additional damage to the DOR Network including PCs and Servers.**

Security Best Practices for System Administrators

Authentication and Authorization (cont'd)

Do not login with your Administrator account to reduce risk to the Revenue information systems.

- **If absolutely necessary that you must login with your administrator account:**
  - **Don't search internet**
  - **Don't use email**

Security Best Practices for System Administrators

Authentication and Authorization (cont'd)

- **If you are currently using an account that has administrator rights and do not have a regular user account, you will be provided with a regular user account.**

- **You should always use your regular user account when logging into the PC to perform your daily tasks such as searching the internet and mail. Only use your administrative privilege account when absolutely necessary. To run executable for example use the "run as a different user".**

Evaluate Function

Evaluate – Revenue staff responsible for evaluation activities (e.g., testers, security analysts).

Role-specific security best practices affecting person with the "Evaluation" role as defined in NIST 800-16.

Security Best Practices for System Testers and Security

- Check sources like SANS , www.sans.org, for listings of common security vulnerabilities and recommended testing methods.

- **Client Security**
  - Pay close attention to applications that have cookies.
- Verify the application uses the most secure version of Transport Layer Security (TLS) to encrypt user name and password or any sensitive information on all communications.
  - Verify the navigational integrity of our web applications.

Source: SANS GIAC paper – Security Testing of Web Applications Best Practices and Tools.

Security Best Practices for System Testers and Security

Client Security - cont'd

- Crashes may leave sensitive information (in cookies) stored on the hard disk.
- Testers should check that cookies and other residual data is periodically sanitized (removed).
- Test that application works with all browser types, versions, client-side security settings.
- Signing code is a suggested best practice for web application integrity.
- Code signing or content signing assures prevention of code tampering.
- Verify that code signing is being performed to ensure web application integrity.

Security Best Practices for System Testers and Security

- **Web Server Security**

  Testers should:

  - Validate input values from the web server side as well as the client side.
  - Validate that files or resources do not contain sensitive information.
  - Verify that the application doesn't store passwords in log files.
  - Validate that confidential data is encrypted.
  - Determine how the application handles expired or revoked certificates.

Security Best Practices for System Testers and Security

- **Web Server Security cont'd:**

  Testers should:

  - Determine if all the services and features which are turned on are required for the application to function.
  - Turn off unnecessary services/ports.
  - Get a list of all open ports, and suggest removal of any unused ports.

Insider Threats

IRS Requirement

The Required by the IRS in Publication 1075 in Section 9.3.2.2.

- *Agencies are required to "*include security awareness training on **recognizing and reporting potential indicators of insider threat**."

Insider Threat Defined

Insider Threat – Have or had authorized access to an organization's network, system or data **and**;

Intentionally

exceeded or misused that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or Resources.

OR

Unintentionally

compromise or potentially compromise NCDOR's ability to accomplish our mission.

Types of Insider Threats & Crimes

Below are the categories of Insider Threats:

- **Intentional**
  - Theft of Intellectual Property (IP)
  - IT Sabotage
  - Fraud
  - Espionage

- **Unintentional**
  - *Accidental Insider Threats (e.g. unauthorized disclosure of Confidential data)*

Theft of Intellectual Property

Theft of IP:

- Intellectual Property thefts are usually committed by current or former employees who have created innovations using employer's resources making it the property of their employer.
- Examples of intellectual property taken may include:
  - Engineering drawings
  - Scientific formulas
  - Source code
- Research shows most insiders steal IP within 30 days of resignation.

Theft of Intellectual Property

Practical monitoring tactics to detect IP thefts:

- Movements of unusual large amounts of proprietary data
- Alerting on emails
- Monitoring network flow data
- Use of host-based agents to log activity
- Implementing targeted auditing of logs

IT Sabotage:

IT Sabotage:

These are crimes in which the insider intended to cause harm to the organization or to individuals.

These crimes are usually committed by disgruntled system administrators or database administrators who often bring down systems, wipe out data or disrupt business operations.

Tactical Methods:

–Backdoors accounts

–Malicious code

–Password crackers

–Social engineering

Insider IT Sabotage (cont'd)

- Key Monitoring and Detection Tactics:
  - **Detection of configuration changes** – Many insiders plant malicious code in operating system scripts, production programs or system utilities.
  - **Perimeter controls to alert on suspicious traffic** Most organizations use tools like intrusion detection systems (IDS) to monitor inbound traffic.
  - **Monitoring for unauthorized accounts** – Many insiders create backdoor accounts for attacking following termination. These accounts can be difficult to detect.

Fraud

- **Insider Fraud**:
  - These are crimes in which an insider uses IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain or theft of information which leads to fraud (identity theft, credit card fraud).

Espionage

- **Espionage**: The practice of spying or using spies, typically by governments to obtain political and military information.

  Although we are not a federal agency, we are still a government agency and could be at the risk for the insider threat of espionage.

Accidental Insider Threat

- Unintentional or Intentional
- Disclosure of confidential information
- Confidential information: Watch email addresses and attachments
- Mistakes
- Loss or degradation of resources
- Jeopardize agency mission

Report Insider Threats

- **Reporting:** It is very important to report any real or suspected Insider Threats to the Service Desk (who will forward these reports to our Information Security Division).

Objectives

At the end of this module, you should be able to:

- Explain the importance of Role-based Security for Technical Users
- Identify the required target audience
- Describe the technical security policies
- Define training based on your job role or duty
- Provide Tips for Detecting Insider Threats

Questions?

David Roseberry
Chief Information Officer
(919) 754-2002

Jerome Smith
Information Security Manager
(919) 754-2395

Rosita Lee
Info. Security Compliance Officer
(919) 754-2418

Credits

Restart